14th ICCRTS

"C2 and Agility"

Title of Paper: **A General Framework of Human Trust in Networks**

Topic(s):
Topic 2: Networks and Networking
Topic 5: Experimentation and Analysis
Topic 10: Collaborative Technologies for Network-Centric Operations

Name of Author(s)

Kevin S. Chan
Natalie Ivanic
Brian Rivera
Elizabeth K. Bowman

Point of Contact: Kevin S. Chan

Name of Organization: ARL-CISD

Complete Address
AMSRD-ARL-CI-NT
2800 Powder Mill Road
Adelphi, MD 20783

Telephone: 301-394-5640

E-mail Address: kevin.s.chan@arl.army.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A General Framework of Human Trust in Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Research Laboratory -CISD,AMSRD-ARL-CI-NT,2800 Powder Mill Road,Adelphi,MD,20783**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
In Proceedings of the 14th International Command and Control Research and Technology Symposium (ICCRTS) was held Jun 15-17, 2009, in Washington, DC

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**32**	

A General Framework of Human Trust in Networks

Abstract

In order to achieve the Army's vision of network centric warfare (NCW), Soldiers must effectively and efficiently interact with tactical networks to maintain information dominance and complete mission objectives. Soldiers must possess a sufficient amount of trust in networks for adequate mission performance. We are investigating human trust in tactical networks by establishing a theoretical framework for analysis and an approach for validation of the framework. We identify reliability and availability as network parameters that define the relationship between quality of service performance and human trust in networks. A general framework is being developed for human trust in networks, which combines singular elements of trust that results in a composite measure of trust. We also present experiments simulating mission scenarios that require situational awareness that will test the validity of the human trust framework. First, we examine the effect that the variation of a single network parameter has on the behavior of human trust in network. Second, we propose similar experiments to determine human trust in network behavior to verify the composite network parameter concept. With proper modeling of such relationships between humans and tactical networks, optimal network design with respect to network utility to the Soldier is possible.

1. Introduction

In network centric warfare operations, it is necessary for Soldiers to be given access to information from a wide-range of sources, and with this information, be able to perform mission objectives in a highly effective and accurate manner. In addition to radio communications with other Soldiers and their superiors, Soldiers have access to other platforms operating in the network, such as unmanned platforms (aerial and ground vehicles, ground sensor) data feeds, satellite imagery, and other information repositories. These sources of command and control (C2) information are passed to the Soldier through situational awareness (SA) tools, such as Command Post of the Future (CPOF), and Force XXI Battle Command, Brigade-and-Below (FBCB2). The Soldier has potential access to the nearly limitless amount of information and is able to make accurate, informed decisions. However, having vast amounts of information to process inherently limits one's efficiency to act.

One area of active research is the design of networks and associated network centric warfare technologies to enable the Soldier to have access to information that is appropriate and timely. This research is directed towards increasing bandwidth/throughput and maximizing display resolutions while minimizing error-rates which directly affects the users view on trust of the performance of the network. Other challenges include data fusion and data reduction techniques for optimization of the use of communications links. In general, these challenges are found in the realm of communication networks design.

The fundamental principles of an emerging science of networks are explored for the military by the National Research Council [NRC, 2005]. The application of network science to the tactical military domain is a recent initiative undertaken by the US Army Research Laboratory (ARL) Army Science Objectives (ASO), which is interested in the relationship between the Soldier and the tactical network. One interest of this effort is to identify the impact of social and cognitive factors of network users on the design of network centric environments. With an idea or model of the dynamic relationship between the Soldier and the tactical network, it may be possible to incorporate such findings into subsequent design of networks. Specifically, we look at a trust metric of the Soldier on the network and identify its varying trust as a function of several parameters, including time and network quality of service.

This paper provides an approach of the influence of cognitive factors the design of tactical networks from the perspective of human trust in networks (TiN). This paper is comprised of several sections. Section 2 discusses the general research problems and motivations for this work. Section 3 summarizes related research found in several different disciplines. Section 4 introduces the general framework by which human trust in networks will be analyzed. Section 5 contains an explanation and results of an empirical test to examine user trust in video with varying quality. Section 6 discusses future directions, and Section 7 is the conclusion.

2. Research Problem

In this section, we identify research problems pertinent to the social and cognitive influence of network design aspect of the network science research initiative. The problems of interest deal with the merging of the dynamics of human trust with the network design and optimization process. Each of the individual areas of human trust and network design has received significant attention, while the composite relationship is not well established.

It is important to distinguish the social and cognitive impact of network design from the study of social networks. The study of social networks uses a model of social relationships to analyze the structure of these associations to draw inference about the dynamics of a community. Typically, a communications network is comprised of nodes representing people and edges representing a certain relationship between two nodes meeting a defined set of criteria. In fact, trust between two parties is a potential criterion. However, the direction of this paper is to analyze the relationship of the interface of a user with a network.

Determining models of social and cognitive relationships for network users is necessary for the optimization of networks to maximize utility to the user. While it is necessary for communications networks to be able to operate at a high quality of service, these technologies are of no utility to the user should the Soldier have a low or no trust in the network. Without trust, the Soldier will simply not use or trust any information from the particular source. In terms of communications networks, the study of the aspects of the physical layer and network layer in networks has received significant attention and resulted in an increased understanding of these issues. The cognitive impacts on network design have not been investigated in simultaneous consideration. As shown in Figure 1, there is a greater level of understanding of the physical and communications aspects of the network, while there is a lesser understanding of the influence of information theory and social and cognitive aspects relating to network science [Swami, 2008].

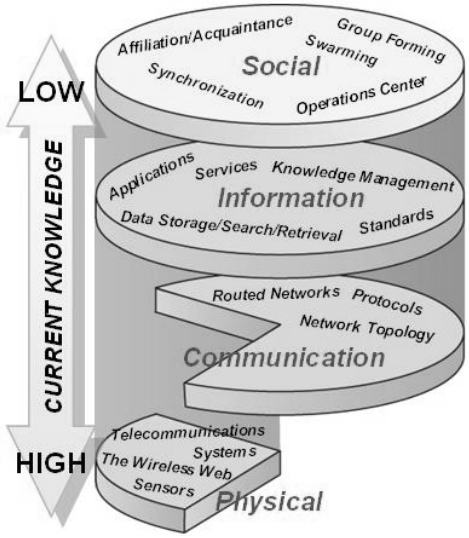


Figure 1: Network Science Layer Stack *[R. Hasenauer 2008]*

3. Related Research Areas

This paper establishes a framework to study the relationship of the user's trust of the network. There are several areas of research to which trust in networks is related. We briefly discuss several related works concerning to trust in automation, situational awareness and military decision making.

In terms of trust in automation, we consider human trust in networks to be a similar problem of interest. Lee [2004] surveys the definition of trust and presents a model for the dynamics of trust in automation. Several concepts related to trust in automation are described. One concept discussed by Lee is the misuse and disuse of automation. Misuse failures are the inappropriate reliance on automation (i.e. ``over" trust), and disuse failures are the rejection of the capabilities of automation (i.e. ``under" trust). The definition of trust is adopted from the related research area of trust in automation. As stated by Lee, trust can be defined as "*the attitude that an agent will help an individual's goals in a situation characterized by uncertainty and vulnerability.*" (page. 54) Also, the notion of trust is examined in structured and dynamic situations, where trust is a critical factor in increasing productivity among organizations. In stable, structured environments, trust is less important. Hierarchical organizations place an emphasis on order and stability minimize transactional uncertainty [Moorman 1993]. Organized structures reduce uncertainty, resulting in appropriate well-defined reliance and generating collaborative advantage [Baba 1999]. Trust facilitates decentralization by making it possible to replace fixed structures and procedures. This concept exposes a conflict in warfighting operations as historical chain of command structures maintain a very structured organization, while network centric operations promote a highly dynamic network structure. Resolving this conflict may be a potential area of interest in TiN.

Lee [2004] also develops a model for the composition of trust, which is comprised of three concepts: appropriateness of trust, the influence of context, and the characteristics of the agent. The evolution of trust (over time) is a result of a feedback system involving these components. Appropriate trust measures the match between the trust and true capability of the automation (calibration of trust). Identification of over trust and distrust are outcomes of this analysis. Contextual trust is governed by individual, cultural and organizational components, contributing to the initial trust in addition to the evolution of trust. The basis of trust considers automation methods that result in varying levels of abstraction of trust in the automated system. Three levels of trust are generalized, network and partner [McKnight 1998]. It is stated that the interaction of these three trust concepts are not well distinguished from each other. The notion of the modeling of composite trust is a current element of our research. In terms of the dimensions of trust, or those factors affecting trust in automation, Lee classifies them into three categories of goal-oriented characteristics: process, purpose, performance. Lee includes a list of dimensions of trust from other existing works.

There are also many studies investigating modeling and measuring trust in automation. Trust combines with other attitudes (workload, effort, risk, self-confidence) to form the intention to rely on automation. It is noted that the type of automation potentially affects the observation of the dynamics of trust [Parasuraman 2000]. There is a difference between automation for reliance (operators act when the automation fails to provide indication that the process is functioning

properly) or for compliance (system indicates when system is not functioning properly [Meyer 2001]. It is also mentioned that trust in automation being modeled as a closed-loop feedback process needs to be studied further.

Faults in automation have been studied, where the trust over time is analyzed [Lee, 1992; Lee, 1994; Itoh, 1999]. Itoh analyzes the trust in an automated process that exhibits two varieties of malfunctions, burst and distributed over time. The main conclusions of this paper are that the occurrence pattern of system malfunctions affects the dynamics of trust and there is memory on the reestablishment of trust. Analyzing the effect of varying performance of the network is an area of investigation for our work.

Additionally, the classical work of Boyd [Boyd 1987] is related to our interest in TiN. This work introduces the OODA (Observe, Orient, Decide and Act) Loop, which is a concept applied to military decision making. This is a closed-loop feedback system that models the cognitive process of a Soldier. It is intended as an optimization on executing this cycle quickly to create a decision making advantage over adversaries. Endsley [2000] provides foundational work on situation awareness and the cognitive process involved with information gathering in various scenarios.

Lastly, we also consider video to experiment with the general framework of trust in networks that is presented in this work. There exist many perceptual studies of varying quality of video and the reaction from those extracting information from these videos [Chen, 2006; Ghinea, 1998; Ghinea, 1999; Gulliver, 2007; Webster, 1993]. Specifically, there is understanding that, despite a reduction in the quality of service of the video, the user is able to still extract information from these videos with some level of performance. The reduction in quality of service is due to degradation factors such as jitter, bit-error rate, and reduced frame rate. Additionally, some order of preference between different degradation factors is established. In terms of trust in networks, we are interested in the way in which the degradation influences the user's trust.

3. Specific Research Areas

We have identified three areas into which this work is divided: modeling dimensions of trust, development and testing of experiments to validate trust models, and specifying approaches to optimize networks based on these trust models. The contribution of this paper is a model identifying a framework to model dimensions of trust in networks and a preliminary test to quantify the dynamics of trust of networks from the perspective of video in the presence of noise. Establishing a greater understanding of the composition and interaction of these three research areas is the ultimate goal.

Dimensions of trust: We present a framework that includes two parameters with which the performance of a network affects the trust of the user. These two parameters are network availability and network reliability. There are models and concepts from trust in automation (TiA) research that are adapted to our investigation in human trust in networks (TiN). It is possible that from TiA work, that the proposed trust framework may need refining or expanding the parameters for which human trust in networks are dependent upon besides availability and reliability.

We also consider several concepts related to the framework of human TiN. A very difficult problem to consider is the idea of composite trust in networks. It is reasonable to evaluate the dynamics of the trust in network from the perspective of one network parameter. However, it is quite evident that trust in networks is a function of multiple parameters. Composite trust is the measure of the dynamics of how overall user TiA evolves as a function of multiple parameters. We also expand the concept of TiA to consider elements that are specific to the networking environment. While in general, the TiA model is appropriate for TiN, we identify characteristics of this type of human-machine interaction that distinguishes TiN from other forms of TiA. Additionally, we also propose to investigate the composite relationship of trust to establish a general notion of human TiN. We are also interested in the evolution of human TiN over time, possibly having network malfunction or failure affect TiN. This examines the degradation or improvement of human trust in the system as a function of time. In TiA, models have claimed that human trust evolves in a manner analogous to a closed feedback loop control system, which is a possible direction of investigation with regard to TiN. The underlying goal of this research is to generate a quantifiable model of the dimensions of human trust that considers necessary network parameters and is able to track the temporal dynamics of human trust.

Trust Experiments: To verify the proposed framework for human TiN, we propose a series of human-in-the-loop experiments. These experiments are generated to establish quantifiable relationships of the human trust and the network performance. It is necessary to analyze the evolution of trust for each of the reliability and availability attributes as a function of those network parameters that affect each of the human TiN. Additionally, the dynamics of composite trust must be evaluated. With these models, it will be possible to estimate human TiN given specific network quality of service or networking parameters present in some scenario. We have identified several areas of investigation in the experimentation process in which we are interested. With particular experimental or actual mission scenarios, it is necessary to determine acceptable approaches and strategies to query user performance and TiA while obtaining quantifiable results. Currently, the optimal approach is not known in terms of the frequency of querying, the specific questions to ask, and the metrics to evaluate the questions.

We developed and ran an experiment to evaluate one aspect of the framework for human TiN. Users were shown video of varying quality and asked to extract certain information from the video. This experiment was able to look at the user performance and preference as a function of error rates.

Network optimization: With accurate models of the human trust in networks, the design of tactical networks can be adjusted to optimize its TiN to the Soldiers. For instance, it may be possible to adapt these TiN models for use as the criteria for establishing routing tables in routing protocols. Ultimately, with the TiN model, we are interested to determine if bounds on TiN are attainable with the adjustment of network parameters. Also, we are interested in identifying tradeoffs with respect to TiN when encountering various networking environments. This is a longer term goal of this research effort.

4. Human Trust in Networks Framework

We have identified human trust of the network as being described by two network attributes: availability and reliability. In terms of availability, some networking factors which affect this notion are connectivity, channel access, and data latency. For reliability, there are issues of data security and data accuracy which affect this attribute. For each of these attributes and the associated underlying factors, their performance affects the human perception of the network. For example, for a Soldier attempting to access a situational awareness server, how does his trust in the network diminish each time he is unable to access the server because of failed or delayed connectivity? Developing a measurable framework for the analysis of the relationship between networking performance and human perception of the network is an important goal of this research.

4.1 General Human TiN Framework

In this section, we present the general framework for human trust in networks. Human TiN is comprised of a user's trust in the availability and reliability in the network. This trust evolves with time and is a function of the changing network quality of service metrics. The TiN framework is a derivative from work in TiA. For instance, our dimensions of trust in the network are reliability and availability. Also, our overall trust in automation (trust in networks) is represented by $\boldsymbol{T_{human}}$.

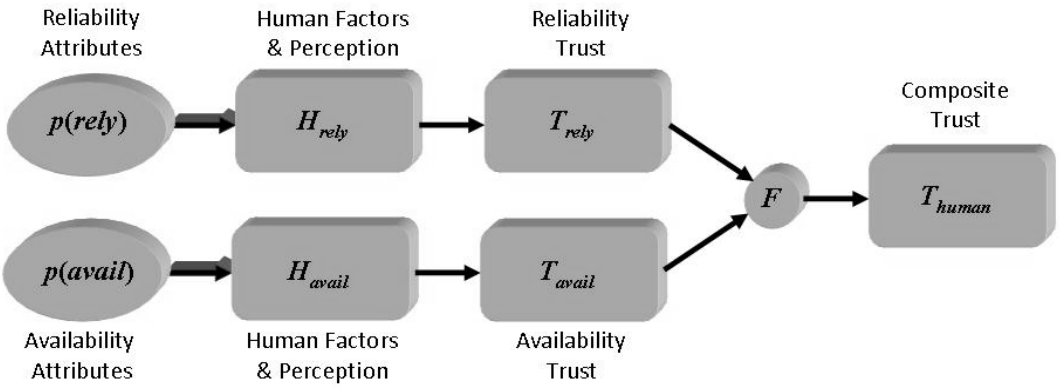


Figure 2: Framework for the analysis of human trust of networks

This framework can be used to analyze the human perception of trust on a network is shown in Figure 2. There is a set of network performance factors that figure into a networking attribute of trust such as network reliability, $\boldsymbol{p(rely)}$ or availability, $\boldsymbol{p(avail)}$. One aspect of this framework is user reaction to changes in network performance of some network factor $\boldsymbol{x}$ with respect to a network attribute, which is represented by $\boldsymbol{H_{p,\,x}(p(\,x))}$. For example, one relationship that exists is the way in which packet delay, $\boldsymbol{p(avail,\ delay)}$, affects the trust of a user in terms of network availability, $\boldsymbol{H_{avail,\ delay}(p(avail,\ delay))}$. We note that there are several network factors that

contribute to a composite trust in a particular network attribute, such as availability. This is illustrated in Figure 2 by the multiple arrows. Additionally, the network factors influencing availability and reliability are not necessarily disjoint. Table 1 is a list of potential network attributes and associated factors for the human TiN framework.

The dynamics of how $\boldsymbol{H_{rely}}$ is established from multiple $\boldsymbol{H_{rely,x}}$ metrics is one area of interest. As in Figure 2, we represent the combined human trust with respect to reliability when considering both data security and data accuracy, $\boldsymbol{T_{rely} = f(H_{rely,\,sec}(p(rely,\,sec)),\, H_{rely,\,acc}(p(rely,\,acc))}$. This is one instance of composite trust in this framework. Additionally, a second instance of composite trust occurs when evaluating trust with respect to network reliability and network availability, which establishes an overall human trust in the network, $\boldsymbol{T_{human} = F(T_{rely},\, T_{avail})}$. It will be important to describe how these different measures of trust are brought together. This is the concept of composite trust.

AVAILABILITY	RELIABLITY
• **Connectivity** Routing protocols Servers in network Network topology Security/access control • **Channel Access** MAC protocols Network traffic • **Data Latency** MAC protocols Hop distances Node density	• **Data accuracy** Synchronization of servers Current, up-to-date data Signal-to-noise ratios • **Data Security** Data integrity Authentication Validation

Table 1: List of network attributes and associated network factors

4.2 Network Centric Operations Specific Requirements

In addition to this framework, there are several characteristics to TiN that are not inherent in TiA work. Furthermore, there are issues specific to the Warfighter that we must also consider. Below are three components of the TiN major areas of interest.

Multiple users: In current TiA work, the majority of the work considers single users. Classical TiA studies airplane pilots and their reliance on cockpit instruments as opposed to visual cues. In a network centric operation, there are multiple users interfacing with the network. At any point in time, each user may have a direct influence on any other user in the network or on the network performance itself. This work has obvious overlap with trust studies in teamwork or supervisor/employee relationships [Tan, 2000; Nyhan, 2000].

Equilibrium state: Given network operations in the battlespace, it can be expected that each Soldier has a significant amount of training in using the network and its available services. Potentially, the human TiN is at a steady state, where any variation in the network QoS has little effect on the human TiN. In addition to having significant amounts of training, Soldiers within the military chain of command have a specific set of protocols to adhere to, limiting the possible uncertainty in certain decision-making scenarios. When given situations of uncertainty, it is expected that the subjective decision-making process is well-matched with those in the objective process. This is captured in Boyd [1987].

Mission-specific information: Soldier TiN may vary for the same network platform for different information or mission requirements. This behavior will require the TiN model to accommodate multiple TiN behavior for each attribute, depending on the information requirements. For example, packet delay will have a varying effect on Soldier trust in the network for various communications media, such as voice or text messages. Ghinea [1999] determines a difference between audio and text in the quality of performance given the same quality of service with respect to packet delay. The quality of performance is an objective method to quantifying trust in networks. Additionally, the TiN given the mission scenario will vary. Mission completion timeliness and perceived threat are two such factors that define the mission scenario.

5. Video Experiments

To verify the TiN framework established in the previous section, we developed a video experiment. This experiment considers the performance and preference of the user as a function of one network factor pertaining to the reliability of the network. The test was developed using the graphical user interface design tool GUIDE in MATLAB, and the videos were obtained through youtube.com (`http://www.youtube.com/user/3rdID8487`). The tests were administered to colleagues at the US Army Research Laboratory. The purpose of this test is to develop a preliminary test that evaluates the TiN with respect to networks with varying block-error rates in a simulated environment.

In this experiment, we present the user with a video of a UAV surveillance feed that shows several moving subjects in the frame. Additionally, the video was degraded in quality in an arbitrarily selected manner. We inserted noise or a block-error rate into the video probabilistically, where a block of 8×8 pixels was affected with probability, ***p***. The block error rate was simulated by converting the grayscale color value of the entire block to be the value of the pixel found in the lower-left hand corner of the block. In total, there were **5** different videos and each of these videos were degraded with ***p* = 0.0** to **0.5** in increments of **0.1**. This resulted in 30 videos, where the order of the videos was randomly presented to the user. Figure 3 shows a screen capture of one of the videos, each with three different error rates: **0.0**, **0.2**, and **0.5**. In the test, users were asked two questions after each video:

Question #1: Identify the number of moving subjects in the presented video.

Question #2: Does the quality of the video give you acceptable information to extract the necessary information requested?

Figure 3: Screen captures of video of varying quality

The intention of this video test is to study the variance of trust with the variance of video quality caused by degrading channel quality. If the video quality were to degrade, it is expected that human TiN would degrade. As evident in [Ghinea, 98; Webster, 93], users can still extract information from video of diminished quality. The behavior that we are interested in is the varying trust in the value of the video with diminished quality. Furthermore, we are investigating the mismatch between the varying trust and ability to extract information from video of varying quality. This relationship has not been studied previously. So, according to the framework in

Figure 2, the $\boldsymbol{p(avail)}$ is the video with some $\boldsymbol{p}$, and $\boldsymbol{H_{rely}(p(rely))}$ is the user's trust in the video with a specific $\boldsymbol{p(avail)}$.

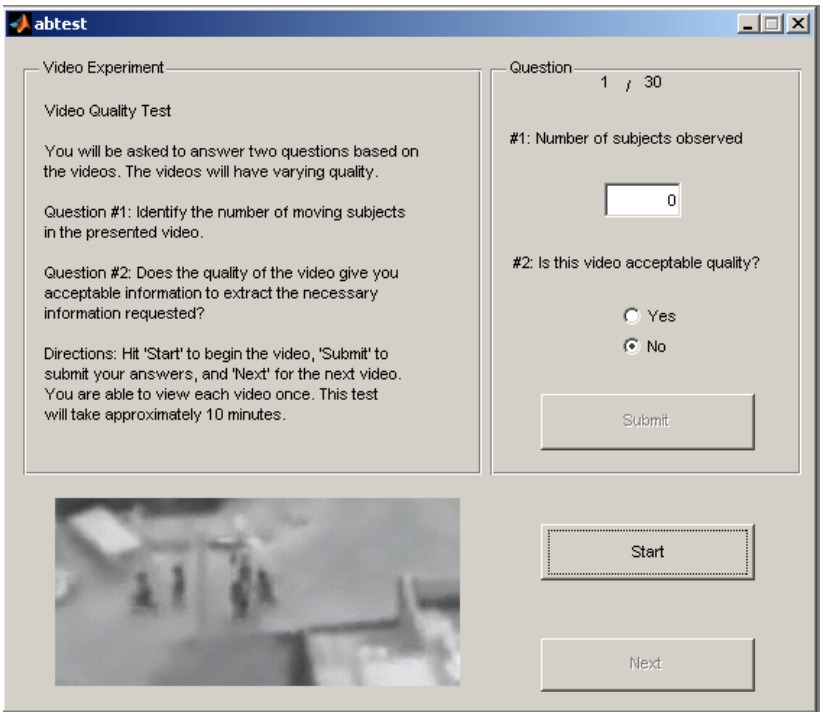


Figure 4: User interface of video experiment

6. Preliminary Results of Video Experiment

We present some results and observations from the video test experiment. First, we discuss some observations and comment on the results of these experiments. Then, we show several trends of the user's responses.

6.1 Experimental Testing Observations

In observation of those taking the video test, there were some consistent reactions and comments. First, there were only 5 unique videos in the test, and user's stated that they were able to recall the number of moving subjects in the video snippet, even if the quality of the video did not allow them to accurately count. Therefore, in this test, there existed a learning behavior to the responses. This would have affected the results of the test from the standpoint that responses from subsequent occurrences of the same video would have an inflated percentage of correct answers. This is considered in Section 6.2.

In terms of the videos used, they were existing degradation in the quality because of the original quality coming from the UAV cameras used to record the feed or the methods used to post them

online. This may affect the analysis of the perceived degree of degradation in the videos, as ***p*** in the videos may be higher than initially stated.

Also, many of those taking the test suggested improvements for the user interface.

- Add a training set.
- Give more choices than Yes/No.
- Allow user to submit "I don't know how many subjects there are."
- Some used prior knowledge, some did not.
- Add drop down selections for answers.
- Increase the size of the video.
- Cross-hairs on the display were distracting.
- Subjects not in the video for the entire duration were difficult to identify.
- Create better database of videos to use in test.

6.2 Video Test Results

In analysis of the user responses of the test, we compare the percentage of correct responses to Question #1 and the percentage of "Yes" responses to Question #2. So, this establishes the comparison between being able to extract the required information from the video (number of moving subjects) with the user's response in terms of their perception of the quality of the video. This result is illustrated in Figure 5. In this figure, it is apparent that despite the user's ability to answer the question correctly, their perception of the video quality diminishes much quicker than their ability to correctly respond. Moreover, these two results indicate two measures of the user TiN. There is a subjective measurement of trust in terms of the responses to the question of acceptable video quality. In contrast, there is an objective measure of TiN with respect to block-error-rate in terms of the ability of the user to correctly identify the number of subjects in the video.

Given a specific mission scenario or objective, these two measures of TiN will vary. In some cases, we expect them to be identical. For instance, Soldiers may have requirements to extract a varying amount of granularity in the video to complete certain mission objectives. In these tasks, there may be a range of consequences associated with those decisions, yielding a change in the responses to Question #2. As a simple example, the response to a "Friend or Foe" question would receive different treatment than simply one asking to identify the number of moving subjects. This dynamic with the human interaction with the network is necessary for optimal network design and optimization.

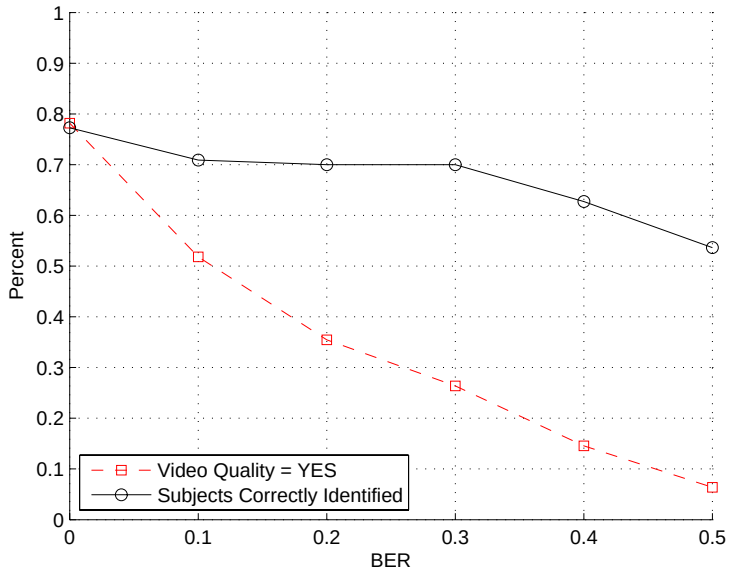


Figure 5: Percent of correct responses and acceptable video quality vs. block error rate

We also tracked the order in which the videos were shown. As stated in Section 6.1, users commented that they were able to use previous knowledge to identify the number of subjects. So, we looked at the percentage of correct responses for each video and for which order they were presented to the user, regardless of ***p***. Figure 6 shows this relationship, and it is also compared against the average percentage of correct responses to Question #1. This result indicates that there is about a 10% increase in correct responses due to learning from the first time the video is shown to the sixth time. Obviously, the variation due to error is eliminated with a larger video database to choose from.

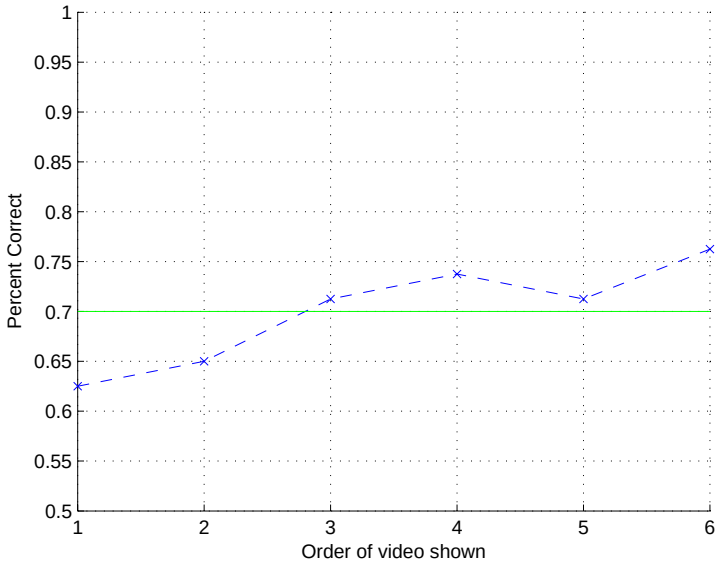


Figure 6: Percent of correct responses vs. the order of video shown

We also looked at the correlation of the responses of the two questions. We considered the each combination of responses and plotted the distribution of the results in Figure 7. The mean along with +/- σ^2 for each of these four combinations of responses are shown. The fraction of correct responses regardless of their perception of video quality reflects an indifference to ***p***, as was also shown in Figure 5. For each of the plots in Figure 7, the statistics are shown in Table 2. Let "✓" indicate "Answer Right" and "Answer Wrong" be denoted by "×".

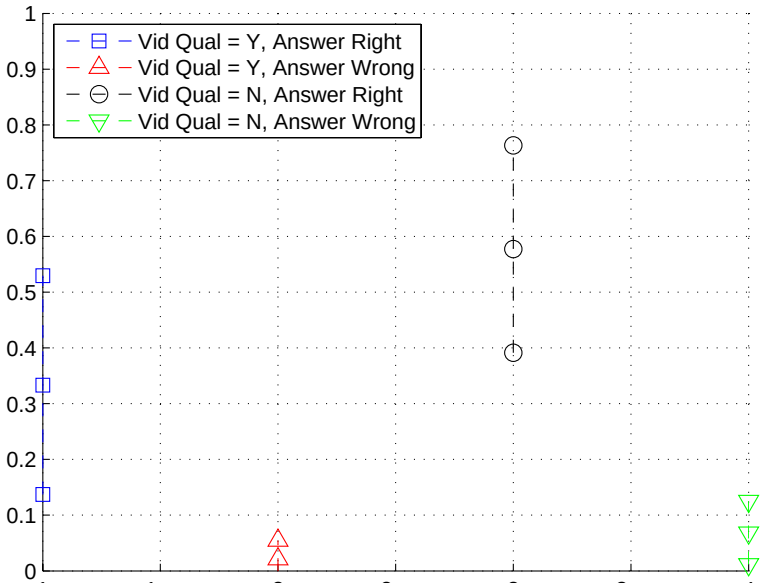


Figure 7: Distribution of responses for the video test

n = 25	Y, ✓	Y, ×	N, ✓	N, ×
mean()	0.33	0.02	0.58	0.07
min()	0.00	0.00	0.23	0.00
max()	0.63	0.13	0.97	.20
σ^2()	0.20	0.03	0.19	.06

Table 2: Statistics on test results for the video test

As these experiments relate to the TiN framework proposed in Section 4, we have established a relationship between the variance of frame error rate to the user trust in reliance. We have seen that there is a mismatch between the perception of allowable video quality and the user's ability to extract information in the video. However, the measure of trust is more likely to follow the trend of the video quality being acceptable versus the ability of the user to extract information from the video. Furthermore, this is even more likely in live mission scenarios as Soldiers will want and require video quality that they deem to be acceptable.

7. Conclusion

We have presented a new framework to model human trust in networks. This trust in networks metric is dependent upon network reliability and availability. Additionally, we have presented results from a video test to measure the perception of video within a given range of network quality of service. This work provides initial results in validating quantifiable models for human trust in networks to enable the design of tactical networks that maximize utility to the Soldier in dynamic networking scenarios.

Bibliography

[Baba 1999] Baba, M. L. Dangerous liaisons: Trust, distrust, and information technology in American work organizations. Human Organization, 58, 331–346, 1999.

[Boyd 1987] Boyd, J. Organic Design for Command and Control, online: http://www.d-n-i.net/boyd/pdf/c&c.pdf, 1987.

[Chen 2006] Chen S., Ghinea G, Macredie R, A cognitive approach to user perception of multimedia quality: An empirical investigation, International Journal of Human-Computer Studies archive Volume 64, Issue 12 (December 2006) 1200-1213, 2006.

[Endsley 2000] Endsley, M. and Garland D., Theoretical Underpinnings of Situation Awareness: A Critical Review. *Situation Awareness and Analysis and Measurement*. Mahwah, NJ: Lawrence Erlbaum Associates, 2000.

[Ghinea 1998] G. Ghinea and J. P. Thomas. QoS impact on user perception and understanding of multimedia video clips. Proceedings of the sixth ACM international conference on Multimedia pp. 49 – 54, 1998.

[Ghinea 1999] Ghinea, G. Thomas, J.P. An approach towards mapping quality of perception to quality of service in multimedia communications, Workshop on Multimedia Signal Processing, 1999 IEEE 3rd pp. 497-501, 1999.

[Gulliver 2007] Gulliver S., Ghinea G. The Perceptual Influence of Multimedia Delay and Jitter. ICME 2007, pp. 2214-2217.

[Itoh 1999] Itoh, M., Abe, G., and Tanaka, K. Trust in and use of automation: Their dependence on occurrence patterns of malfunctions. In Proceedings of the IEEE International Conference on
Systems, Man, and Cybernetics (Vol. 3, pp. 715–720). Piscataway, NJ, 1999.

[Lee 1992] Lee, J. D., & Moray, N. Trust, control strategies and allocation of function in human-machine systems. Ergonomics, 35, 1243–1270, 1992.

[Lee 1994] Lee, J. D., & Moray, N. Trust, self-confidence, and operators' adaptation to automation. International Journal of Human-Computer Studies, 40, 153–184, 1994.

[Lee 2004] Lee, J. and See, K. Trust in Automation: Design for Appropriate Reliance. Human Factors, Vol 46, No. 1, pp. 50-80, Spring 2004.

[McKnight 1998] McKnight, D. H., Cummings, L. L., and Chervany, N. L. Initial trust formation in new organizational relationships. Academy of Management Review, 23, 473–490, 1998.

[Moorman 1993] Moorman, C., Deshpande, R., and Zaltman, G. Factors affecting trust in market-research relationships. Journal of Marketing, 57(1), 81–101, 1993.

[Nyhan 2000] Nyhan, R. C. Changing the paradigm – Trust and its role in public sector organizations. American Review of Public Administration, 30, 87–109, 2000.

[NRC 2005] Network Science National Research Council, Network Science. National Academies Press, 2005.

[Parasuraman 2000] Parasuraman, R., Sheridan, T. B., and Wickens, C. D. A model for types and levels of human interaction with automation. IEEE Transactions on Systems Man and Cybernetics – Part A: Systems and Humans, 30, 286–297, 2000.

[Swami 2008] Swami, A., "Research Center on Communication Networks," online: http://www.arl.army.mil/www/DownloadedInternetPages/CurrentPages/CTA/Documents/conference/2008/OppDay_NS_CTA-Comm_Nets-27Aug2008.pdf, 2008.

[Tan 2000] Tan, H. H., & Tan, C. S. Toward the differentiation of trust in supervisor and trust in organization. Genetic, Social, and General Psychological Monographs, 126, 241–260, 2000.

[Webster 1993] Webster A., Jones C., Pinson M., Voran S., and Wolf S.- SPIE Human Vision, Visual Processing, and Digital Display IV, 1993.

U.S. Army Research, Development and Engineering Command

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

A General Framework of Human Trust in Networks

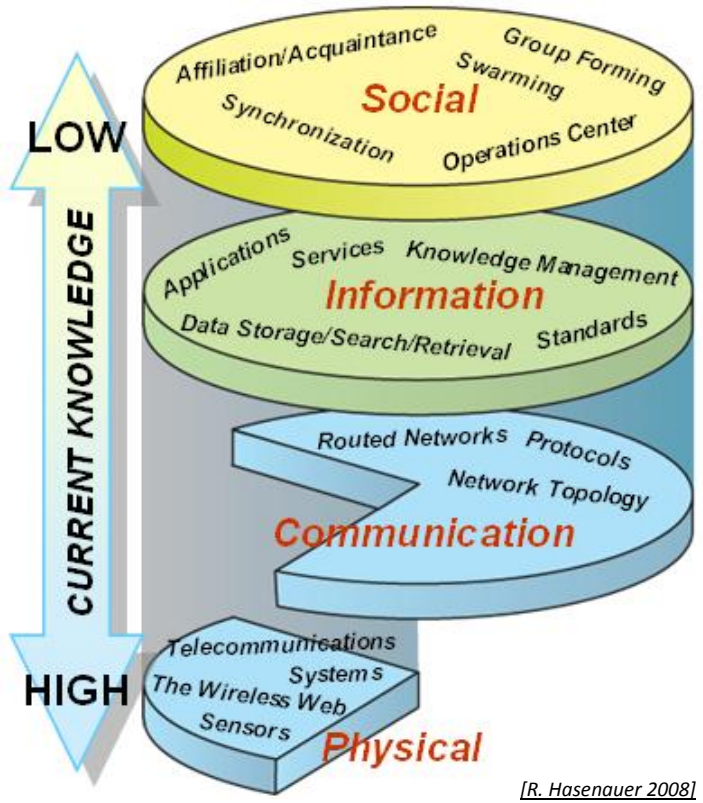
14th ICCRTS "C2 and Agility"

June 15, 2009

K. Chan, N. Ivanic, B. Rivera, E. Bowman

Motivation

- **Motivation:** Build tactical networks that maximize the capability/ability of the Soldier in performing mission objectives.
  - Presently, there is a lack in the understanding of the social/cognitive layers of the network science paradigm.
  - Furthermore, the interconnection of the communications, information and social/cognitive layers must be understood.



[R. Hasenauer 2008]

Challenges

- Specifically, networked devices and information services are a growing capability among the warfighter. However, several challenges arise despite advances in technology:
  - Information overload: The Soldier has access to many multimedia services (video, images, clips, http, chat, UAV feeds).
  - Transfer of information: The chain of command and the dissemination of information are potentially at odds.
  - Collaboration using the network: Soldiers need optimal and efficient capabilities to share and disseminate information.
  - Trust in network: Reliance and confidence in the battle command systems and networked devices is necessary.
- Trust as a metric to evaluate Soldier interaction with the network.

[www.spectrum.ieee.org]

Related Research Areas

- Dimensions of Trust: The ability of the user to gather information of its targeted environment and be able to make decisions based on these observations. The user and decision maker must possess a satisfactory amount of trust in this information.
  - Trust in Automation [Lee 04, Parasuraman 00]
  - Situational Awareness [Endsley 99]
  - Decision-making [Boyd 87]

- Trust Experiments: Validation of the models for human perception of video and dissemination of information is necessary.
  - Video perception studies [Ghinea 98, Chen, 06]
  - Collaboration Experiments [Moorman 93, Baba 99]

- Network Optimization: Many approaches for optimization of network performance using various metrics exist. Human trust in networks is a new metric for optimization.

Approach

Human Trust in Networks

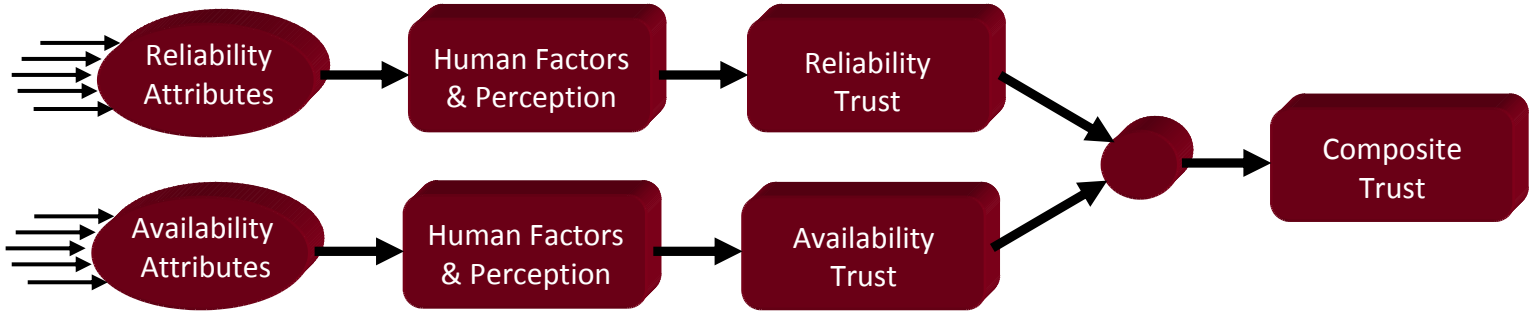
- Develop measurable models for human trust in networks (TiN)
  - Dimensions of trust : Network reliability, network availability
  - Composite trust
  - Quantifiable metrics of human trust vs. network parameters

- Experimental validation of trust models
  - Video tests for Human TiN
  - Preliminary results/analysis

- Determine approaches for network optimization
  - Routing layer: traffic rerouting, network topology optimization.
  - Application layer: information filtering, adaptive priority-based access control and delivery rate.

Human Trust in Networks Framework

General Framework of Trust in Networks



Availability

- → **Connectivity**: Routing protocols, servers in network, network topology, security/access control
- → **Channel Access**: MAC protocols, network traffic/congestion
- → **Data Latency:** MAC protocols, hop distances, node density

Reliability

- → **Data accuracy**: Synchronization of servers, data freshness/timeliness, signal-to-noise ratios,
- → **Data Security:** Data integrity, authentication, validation

Experimental Validation

- Validation using a video test
  - Determine the effect of degradation in the quality of video on the human performance to extract information.
  - Simulate a video stream from a unmanned aerial vehicle.

- One parameter of reliability in the network and its effect on the human trust in network using video.

- Measure objective vs. subjective performance and possible implications on network optimization.

- Preliminary Video Test
  - Varying frame error rate to simulate network QoS.
  - Experiment asked 2 questions/ mission objectives:
    1. Identification of the number of moving subjects, [0, 1, 2, …].
    2. Perception of the video being of sufficient quality, [Yes, No].

- Test Specifications:
  - 5 different video feeds with a variable number of people moving.
  - Range of 'frame' error rate for each video: {0%, 10%, … , 50%}.
  - Order of videos was randomly chosen.
  - Videos were only viewable once.

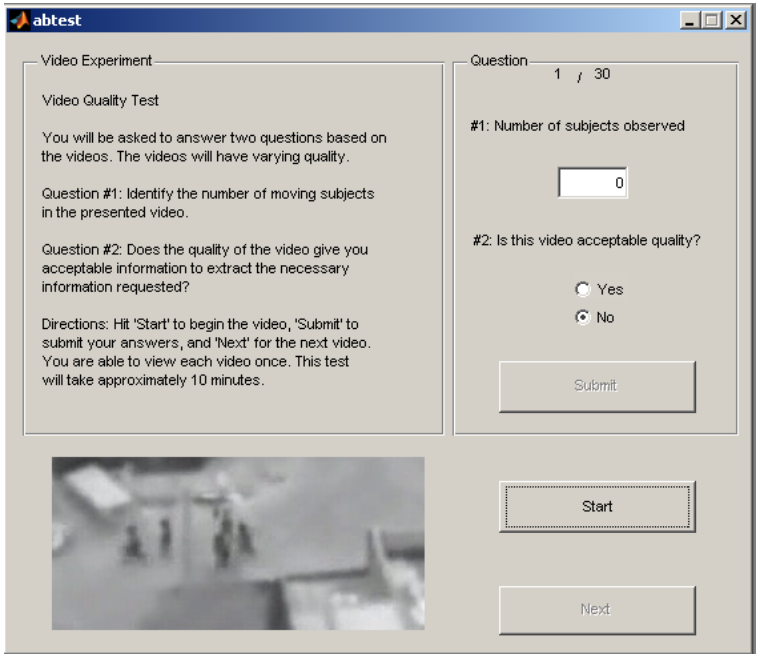
Observations

Experiential

- Learning from previously viewed video.
- Difficulty in identifying subjects that were not in the video for the entire duration.
- Distracting elements of video that were not part of the content (i.e. cross-hairs)

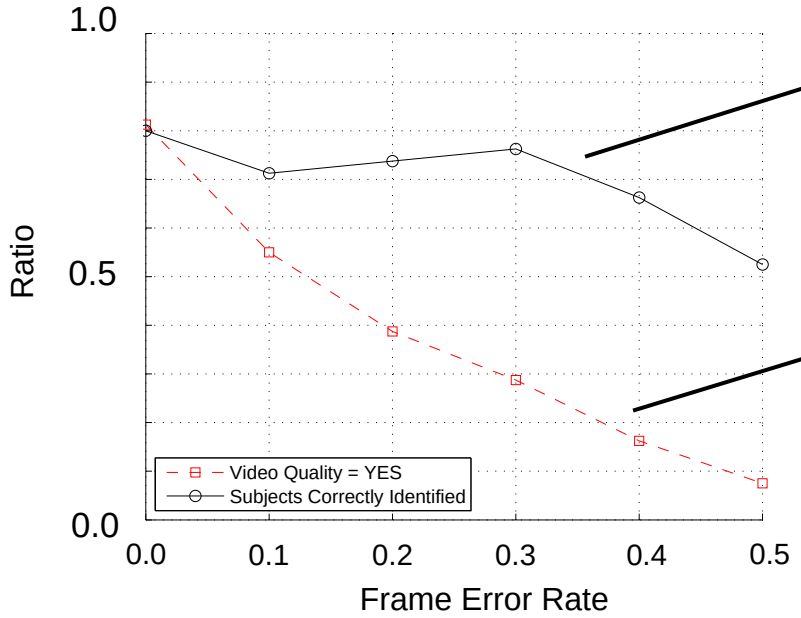
Implementation

- Training set to add familiarity to test.
- Answer submission methods:
  - Multiple choice, Text box
  - Allow user to submit the response “I don’t know how many subjects I see.”
- Increased video resolution.



Video Test Results I

- Results : Plot of the number of correct responses to question #1 and those answering YES to question #2 versus frame error rate.
- Objective measure of performance (subject identification) is maintained despite significant decrease in the subjective measure (acceptable video quality).
- Evaluating Human TiN metrics: Subjective vs. Objective measure.

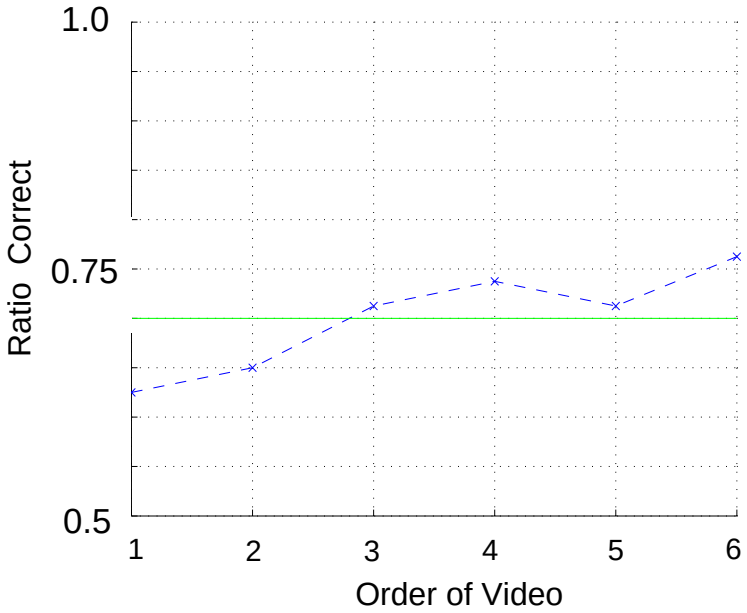


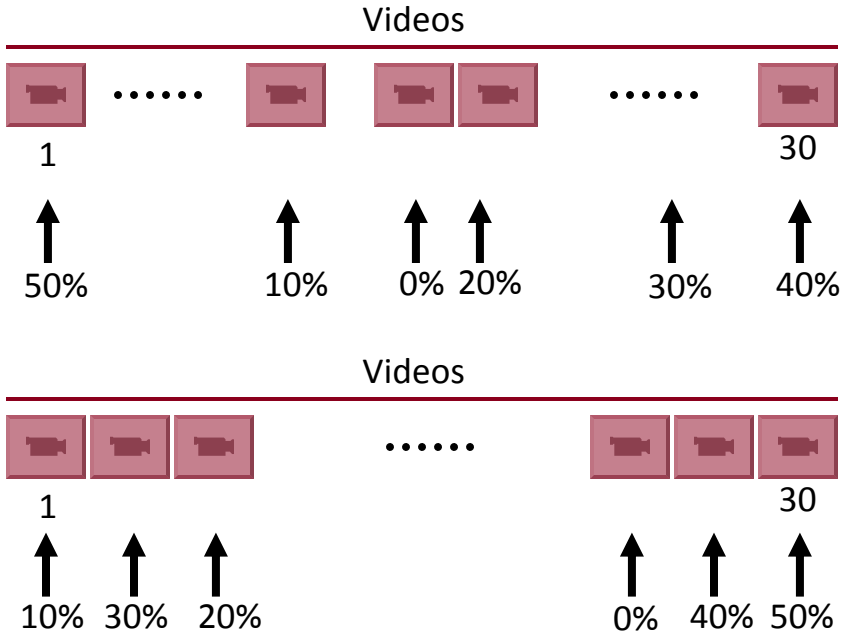
#1: Number of subjects observed: {Correct}

#2: Is this video acceptable quality? {YES}

Video Test Results II

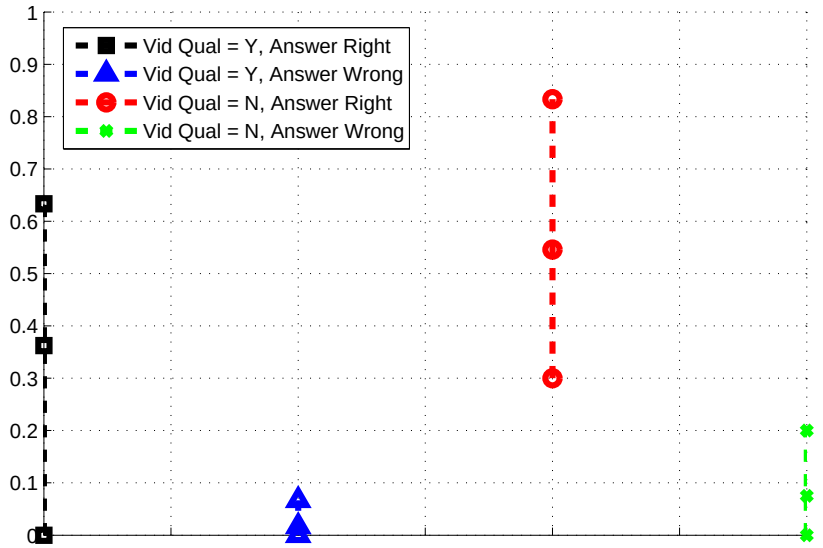
- The order of videos and error rates was randomly selected. Trends in responses exhibit a learning of the content of the videos based on order of viewing.
- From the first showing of the video to the last, there is a 13% (63%-76%) increase in percentage of correct answers.
- Mean of correct responses: 70%





Video Test Results III

- Distribution of the four combinations of responses:
  - {Yes} video quality, {Correct} response
  - {Yes} video quality, {Incorrect} response
  - {No} video quality, {Correct} response
  - {No} video quality, {Incorrect} response
- Statistics on these responses (max, min, mean, std. dev.).
- Results suggest and indifference to the frame error rate.



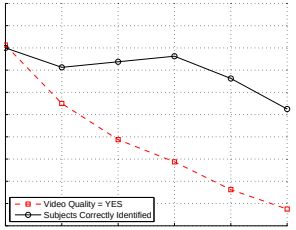
n = 25	Y, ✓	Y, ×	N, ✓	N, ×
mean()	0.33	0.02	0.58	0.07
min()	0.00	0.00	0.23	0.00
max()	0.63	0.13	0.97	.20
σ^2()	0.20	0.03	0.19	.06

Ideas on Network Optimization

- Network Optimization on Frame Error Rate (FER)
  - $Trust_{REL}(FER) = f (FER)$
  - Determine limits on FER to provide sufficient $Trust_{REL}$ for specific scenarios.

- Composite Trust:
  - Analysis using multiple attributes is necessary to establish a composite $Trust_{REL}$.
  - An overall Trust in Networks metric, $Trust_{TOT} = f (Trust_{REL}, Trust_{AVL})$.

$Trust_{REL}$(FER) vs. FER



Research Directions

- **Human Trust in Networks Models**
  - Consider dynamics of **composite trust** and the **time-varying** evolution of human TiN.
  - Establish a classification of mission objectives into the trust model. The **variation of mission objectives** have different requirements and affect associated trust models.
  - **Multiple networked users** and its affect on individual user TiN.

- **Experimental validation of trust models**
  - Build a comprehensive TiN Experiment environment with a multimedia (video/audio/image) database to allow for improved querying techniques

- **Network Optimization for a trusted, reliable and available network**
  - **Routing Layer:** Reroute traffic around a congested/failed node. Restructuring network topology to adapt to specific network environment.
  - **Application Layer:** Filter necessary information to soldier for optimal mission completion potential. Adapt network QoS and access to network services to individual soldiers based on mission completion requirements.

Summary

- A new general framework to measure human trust in networks that is based on network reliability and availability.
- Results of a video test to validate and illustrate the proposed trust framework.
- Possible implementation of the trust framework into network optimization approaches.